THAT WHICH IS CLAIMED IS:

1. A method of generating output bytes corresponding to respective input bytes according to an one-to-one binary function, comprising the steps of

decoding an input byte generating at least a bit string that contains only one active bit;

logically combining the bits of said bit string according to said binary function for generating a 256-bit string representing a corresponding output byte;

encoding said 256-bit string in a byte, obtaining said output byte.

2. The method of claim 1, wherein said second 256-bit string is obtained by carrying out the steps of

subdividing the input byte in a left nibble (L) and a right nibble (R);

decoding the left nibble (L) and right nibble (R) in a left 16-bit string and a right 16-bit string, respectively, each containing only one active bit;

logically combining the bits of said 16-bit strings according to said binary function for generating said 256-bit string.

3. The method of claim 1, wherein

said input byte is decoded in a corresponding auxiliary 256-bit string;

said first 256-bit string is obtained by changing the order of the bits of said auxiliary 256-bit string according to said binary function.

4. The method of claim 1, wherein said one-

to-one binary function represents the ByteSub operation of the Rijndael AES encryption/decryption algorithm.

5. The method of claim 2, wherein each bit of said second 256-bit string is obtained by ANDing among them bits of said 16-bit strings.

6. A hardware device for generating output bytes corresponding to respective input bytes according to an one-to-one binary function, comprising

a decoder of the input byte, generating at least a bit string that contains only one active bit;

an array of logic gates input with said bit string, generating a 256-bit string by logically combining the bits of the input string according to said one-to-one binary function;

an encoder input with said 256-bit string, generating said output byte.

7. The hardware device of claim 6, wherein

said decoder is composed of a left decoder and a right decoder input with a left nibble (L) and a right nibble (R) of the input byte, and generating a left 16-bit string and a right 16-bit string, respectively, each containing only one active bit;

said array of logic gates generates said 256-bit string as logic combination of bits of said 16-bit strings.

8. The hardware device of claim 7, wherein said array of logic gates is an array of 256 AND gates, each generating a respective bit of said 256-bit string by ANDing bits of said 16-bit strings.

9. The hardware device of claim 7, further comprising

an array of multiplexers each input with bits of said 16-bit strings and driven by selection signals and generating a respective intermediate bit fed to said array of logic gates;

said logic gates generating bits of said 256-bit string by logically combining said intermediate bits.

10. The hardware device of claim 6, wherein

said decoder of the input byte generates a corresponding auxiliary 256-bit string;

said array of logic gates generates said first 256-bit string by changing the order of the bits of said auxiliary 256-bit string in input according to said one-to-one binary function.

11. An electronic circuit performing the rijndael aes encryption/ decryption algorithm, comprising a hardware device (s-box) according to claim 6 wherein said one-to-one function corresponds to the bytesub operation of said algorithm.